



KOREAN INTELLECTUAL PROPERTY OFFICE

## KOREAN PATENT ABSTRACTS

(11)Publication number: **1020030049643 A**  
 (43)Date of publication of application: **25.06.2003**

(21)Application number: **1020010079921**  
 (22)Date of filing: **17.12.2001**

(71)Applicant: **ELECTRONICS AND  
TELECOMMUNICATIONS  
RESEARCH INSTITUTE**  
 (72)Inventor: **BAN, SEONG BEOM  
JUNG, YONG HWA  
KIL, YEON HUI  
MUN, DAE SEONG**

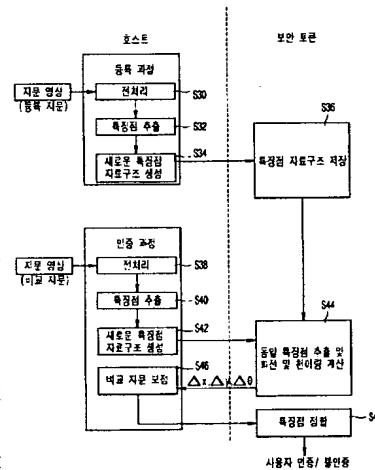
(51)Int. Cl. **G06K 9/00**

## (54) FINGERPRINT RECOGNITION METHOD FOR PERSONAL DEVICE OPERATED WITH LOWER POWER

## (57) Abstract:

**PURPOSE:** A fingerprint recognition method for a personal device operated with lower power is provided to make a host system perform a floating point operation and a multiplication operation for a comparison of minutiae data between registered and input fingerprint or a fingerprint compensation, and to make a personal device, e.g., a smart card or a USB security token, repeat a fixed point operation.

**CONSTITUTION:** The method comprises several steps. A host receives the image data of fingerprint registered by a user, generates minutiae data structure for the registered fingerprint (S30, S32, S34), and registers the minutiae data structure for the registered fingerprint at a personal device (S36). If a user transmits fingerprint image data to the host for a user authentication request, the host receives the fingerprint image data, generates the minutiae data structure, and transmits the minutiae data structure to the personal device (S38, S40, S42). The personal device extracts the same minutiae data between the registered and the newly transmitted minutiae, calculates parameters on a rotation or transition between the two image data by referring to the extracted minutiae data, encodes the calculated parameters, and transmits the encoded parameters to the host (S44). The host compensates for the minutiae data on the newly input fingerprint image by using the transmitted parameters (S46). The host matches the minutiae of the registered fingerprint with that of the compensated fingerprint, and authenticates the user or not according to the matching result (S48).



COPYRIGHT KIPO 2003

## Legal Status

Date of final disposal of an application (20040923)  
 Patent registration number (1004523240000)  
 Date of registration (20041001)  
 Number of opposition against the grant of a patent ( )  
 Date of opposition against the grant of a patent (00000000)  
 Number of trial against decision to refuse ( )  
 Date of requesting trial against decision to refuse ( )

(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(51) Int. Cl.  
G06K 9/00

(11) 공개번호 특2003-0049643  
(43) 공개일자 2003년06월25일

(21) 출원번호 10-2001-0079921  
(22) 출원일자 2001년12월17일  
(71) 출원인 한국전자통신연구원  
대전 유성구 가정동 161번지  
(72) 발명자 문대성  
부산광역시시하구괴정2동190-233/5  
길연희  
경상남도마산시합포구중앙동대동한마음아파트503호  
반성범  
대전광역시유성구지족동열매마을아파트3단지306동1604호  
정용화  
대전광역시유성구전민동엑스포아파트208동603호  
(74) 대리인 권태복, 이화익

실사청구 : 있음

(54) 저전력을 사용하는 개인장치용 지문 인식 방법

요약

본 발명은 저전력을 사용하는 개인장치용 지문 인식 방법에 관한 것으로서,

호스트에서 사용자지문영상을 입력받아 특징점 자료구조를 생성하는 단계(S30, S32, S34)와, 호스트에서 생성된 특징점 자료구조를 개인장치에 등록하는 단계(S36)와, 호스트에서 비교지문영상에 대한 특징점 자료구조를 생성하여 개인장치로 전송하는 단계(S38, S40, S42)와, 개인장치에서 사용자의 특징점 자료구조와 비교지문영상의 특징점 자료구조에서 동일한 특징점을 추출하고, 동일한 특징점을 기준으로 두 영상의 회전 및 전이에 대한 파라미터를 산출하여, 파라미터를 암호화하여 호스트로 전송하는 단계(S44)와, 호스트에서 파라미터에 의해 비교지문영상에 대한 특징점을 보정하는 단계(S46), 및 보정된 비교지문과 등록 지문의 특징점에 대한 점대칭동작을 수행하여 사용자인증을 결정하는 단계(S48)로 이루어지며,

이에 따라서, 하드웨어 자원이 빈약하여 등록 지문과 비교 지문의 특징점을 보정하기 위한 부동 소수점 연산 또는 곱셈 연산을 지원하지 않는 개인 장치에서도 용이하게 적용할 수 있다.

도표도

도2

색인어

지문 인식, 생체 인식, 스마트 카드, USB 보안 토큰, 사용자 인증

영세서

도면의 간단한 설명

도 1은 종래의 저전력을 사용하는 개인장치용 지문 인식 방법의 작동상태를 도시한 흐름도,  
도 2는 본 발명에 따른 저전력을 사용하는 개인장치용 지문 인식 방법의 작동상태를 도시한 흐름도,  
도 3과 도 4는 본 발명에 따른 지문 영상의 기준 특징점과 이웃 특징점 사이의 기하학적인 구조도,  
도 5는 본 발명에 따른 등록 지문과 비교 지문의 특징점에서 동일한 특징점을 추출하는 과정을 도시한 구성도이다.

발명의 상세한 설명

## 발명의 목적

### 발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 지문 인식 방법에 관한 것이며, 보다 상세히는 스마트카드나 USB보안토크와 같이 저전력을 사용하는 개인장치용 지문 인식 방법에 관한 것이다.

일반적으로 지문 인식 방법은 영상 기반의 지문 인식 방법과 특징 기반의 지문 인식 방법으로 구분된다.

상기 영상 기반의 지문 인식 방법은 영상정보를 이용한 방법으로서, 개버(Gaber)필터, 고속푸리에변환(FFT: Fast Fourier Transform), 기울기, 방향성 히스토그램, 투영 등의 기법을 적용하여 지문 영상의 전체적인 방향성 정보를 이용하는 가장 고전적인 방법 중의 하나이다.

상기 특징 기반의 지문 인식 방법은 크게 특징추출(minutiae extraction)과 매칭(matching)의 두 과정으로 이루어지는 가장 보편적인 방법으로서, 평활화, 전경과 배경영역의 분리, 이진화, 세션화 등의 여러 가지 영상처리기법을 적용하여 추출된 특징점(minutiae)들의 공간적인 특징을 이용한다.

한편, 상기와 같은 지문 인식 방법을 저전력을 사용하는 스마트 카드나 USB 보안 토크 등과 같은 개인장치에 적용한 종래의 지문 인식 방법은 스마트 카드나 USB보안 토크에 지문 데이터를 저장만하고 모든 지문 인증 작업이 호스트에서 이루어지는 수준(Store-on-Card)의 제품이 상용화되어 있으며, 스마트 카드나 USB보안 토크에서 지문 인증 과정이 수행되는 방법(Match-on-Card)은 현재 연구되어지고 있으며, 도 1에 도시된 바와 같이 수행된다.

여기서, 도 1에 도시된 지문 인식 방법은 저전력을 사용하는 USB 보안 토크에 적용한 종래의 지문 인식 방법으로서, 스마트 카드에도 동일한 방법으로 적용되며, 이 경우 아래의 호스트 컴퓨터는 카드리더기로 대체된다.

도 1을 참조하면, 제일 먼저 호스트 컴퓨터에서는 사용자 인증을 위하여 등록하고자 하는 사용자의 지문 영상을 입력받아 상기 입력 지문 영상을 전처리하여(S10) 상기 입력 지문 영상으로부터 지문의 특징점을 추출한 후(S12), 추출된 특징점들간의 상대적인 각도차, 상대적인 거리, 용선의 개수 등의 기하학적인 정보를 가지는 특징점 자료구조를 생성하여(S14), 상기 특징점 자료구조를 USB 보안 토크에 등록한다(S16).

상기와 같이 USB 보안 토크에 사용자의 지문 영상으로부터 추출한 특징점 자료구조가 등록된 상태에서, 상기 호스트 컴퓨터로 소정의 지문 영상(이하, 비교 지문 영상)이 입력되면, 상기 호스트 컴퓨터는 비교 지문 영상에 대하여 상기 사용자 지문 등록 과정과 동일하게 전처리(S18), 특징점 추출(S20), 및 자료구조 생성(S22) 절차를 수행하여 비교 지문 영상에 대한 특징점 자료구조를 생성하여 상기 USB 보안 토크으로 전송한다.

이에 따라서, 상기 USB 보안 토크는 기등록된 사용자의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점을 추출하여 추출된 특징점들 사이의 회전 및 전이에 대한 파라미터, 예컨대 비교해야 할 두 지문 영상사이의 회전된 각도( $\Delta\theta$ ), 비교해야 할 두 지문 영상사이의 전이된 좌표양( $\Delta x$ ,  $\Delta y$ )을 산출하고(S24), 산출된 파라미터에 의해 상기 비교 지문 영상에 대한 특징점을 보정한 후(S26), 점매칭 동작을 수행하여 등록 지문과 비교 지문의 일치 여부에 따라서 사용자 인증을 결정한다(S28).

이때, 상기 USB 보안 토크에서는 부동 소수점 연산(Floating-point operation) 및 곱셈 연산을 수행하여 등록 지문과 비교 지문의 특징점을 보정하고 비교하여 사용자 인증 여부를 결정한다.

그러나, 상기와 같이 저전력을 사용하는 스마트 카드나 USB 보안 토크와 같은 개인장치에 적용하는 종래의 지문 인식 방법은 카드리더기나 호스트 컴퓨터에서는 특징점 추출 과정만을 수행하고 스마트 카드나 USB 보안 토크와 같은 개인장치에서 등록 지문과 비교 지문의 특징점을 보정하고 비교하기 위하여 부동 소수점 연산 및 곱셈 연산을 전적으로 수행해야 하기 때문에, 복잡한 연산을 위하여 요구되는 다수의 메모리 등의 하드웨어 자원을 기술적으로 충분히 만족시키기 어려운 문제점이 있다.

또한, 상기 문제점을 해결하기 위해서 개인장치에 저장된 사용자의 등록 지문이 호스트로 전송되어 하드웨어 자원이 풍부한 호스트에서 지문 인증이 이루어질 경우, 사용자의 지문 정보가 쉽게 외부로 유출될 수 있다는 문제점이 있다.

### 발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상술한 종래의 문제점을 극복하기 위한 것으로서, 본 발명의 목적은 다수의 메모리 등의 풍부한 하드웨어 자원을 구비한 호스트에서 등록 지문과 비교 지문의 특징점을 비교하고 보정하기 위한 공지의 부동 소수점 연산 및 곱셈 연산을 전적으로 수행하도록 하고, 스마트 카드나 USB 보안 토크와 같은 저전력을 사용하는 개인장치에서는 고정 소수점 연산(Fixed-point operation)의 반복만으로 지문 비교가 가능하도록 하는 저전력을 사용하는 개인장치용 지문 인식 방법을 제공하는데 있다.

상기 본 발명의 목적을 달성하기 위한 저전력을 사용하는 개인장치용 지문 인식 방법은, 호스트에서 사용자 인증을 위하여 등록하고자 하는 사용자의 지문 영상을 입력받아 전처리하여 지문의 특징점들을 추출한

후, 추출된 특징점들간의 기하학적인 정보를 가지는 특징점 자료구조를 생성하는 단계와, 상기 호스트에서 생성된 특징점 자료구조를 개인장치에 등록하는 단계와, 상기 호스트로 비교 지문 영상이 입력되면 비교 지문 영상에 대한 특징점 자료구조를 생성하여 상기 개인장치로 전송하는 단계와, 상기 개인장치에서 기록된 사용자의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점을 추출하고, 동일한 특징점을 기준으로 두 영상의 회전 및 전이에 대한 파라미터를 산출하여, 산출된 파라미터를 암호화하여 호스트로 전송하는 단계와, 호스트에서 상기 암호화된 파라미터에 의해 상기 비교 지문 영상에 대한 특징점을 보정하여 개인장치로 전송하는 단계, 및 개인장치에서 보정된 비교 지문과 등록 지문의 특징점에 대한 점대칭 동작을 수행하여 사용자 인증을 결정하는 단계로 이루어진다.

#### 발명의 구성 및 작용

이하, 본 발명에 따른 저전력을 사용하는 개인장치용 지문 인식 방법을 첨부한 도면을 참조하여 상세히 설명하기로 한다.

도 2는 본 발명에 따른 지문 인식 방법이 USB 버스 토큰에 적용된 실시예이며, 상기 USB 버스 토큰이 스마트 카드로 대체되면 상기 호스트는 카드 리더기로 대체된다.

도 2를 참조하면, 본 발명에 따른 지문 인식 방법은 호스트에서 사용자 지문 정보에 대한 특징점을 추출하고 개인장치에 특징점 정보를 저장하는 등록 과정과 호스트에서 비교 지문 정보에 대한 특징점을 추출하고 상기 USB보안 토큰에 저장된 사용자 지문과 비교하여 보정에 필요한 위한 파라미터 산출하고, 비교 지문을 보정한 후 두 지문을 정합하는 인증 과정으로 이루어진다.

상기 호스트에서는 부동 소수점 연산과 곱셈 연산을 많이 필요로 하는 등록 과정에서의 등록 지문에 대한 특징점을 추출하거나, 인증 과정에서의 비교 지문에 대한 특징점을 추출하고 비교 지문을 보정하는 동작을 수행한다.

상기 USB 보안 토큰에서는 고정 소수점 연산 및 덧셈 연산만을 반복하여 등록 지문의 특징점 자료구조에 대한 파라미터를 산출하고 사용자 인증을 위한 점대칭 동작을 수행한다.

상기와 같이 이루어지는 본 발명에 따른 저전력을 사용하는 개인장치용 지문 인식 방법은 다음과 같이 수행된다.

최초에, 상기 호스트에서는 사용자 인증을 위하여 등록하고자 하는 사용자의 지문 영상을 입력받아 전처리하여(S30) 등록 지문의 특징점들을 추출한 후(S32), 추출된 특징점들간의 기하학적인 정보를 가지는 특징점 자료구조를 생성한 다음(S34), 상기 사용자의 특징점 자료구조를 USB 보안 토큰으로 전송하여 등록한다(S36).

이때, 상기 호스트에서는 USB 보안 토큰에서 등록 지문과 비교 지문 사이의 동일한 특징점을 추출하여 소정의 파라미터를 산출할 때, 특징점에 대한 탐색영역을 감소시키기 위해서 동일한 지문 영상을 2회 입력받아 특징점 추출작업을 2회 반복하여 얻은 두 지문 영상의 특징점 중에서 공통적으로 존재하는 특징점만을 추출한다.

또한, 상기 특징점 자료구조는 동일한 특징점을 보다 효율적으로 추출하기 위해서 필요에 따라 지문 영상에서 용선의 끝점과 분기점 외에 이웃한 특징점과의 기하학적인 정보를 가질 수 있으며, 특히 본 발명에서는 특징점들 각각에 대해서 가장 가까운 5개의 이웃 특징점들 사이의 상대적인 각도차, 상대적인 거리, 용선의 개수 등의 기하학적인 정보를 가지며, 상기 특징점 추출 및 특징점 자료구조 생성 과정을 보다 상세히 설명하면 다음과 같다.

도 3과 도 4를 참조하면, 상기 호스트에서는 등록 지문 영상으로부터 영상 평활화, 배경과 전경의 분리, 이진화, 세션화와 같은 다양한 영상처리방법을 적용하여 용선의 끝점과 분기점의 좌표값 및 방향정보로 구성된 특징점을 추출하게 된다.

또한, 추출된 각각의 기준 특징점(M)에 대하여는, 나머지 특징점들과의 좌표값에 대한 유클리디언 거리를 구한 후, 이를 오름차순으로 정렬하고, 다른 특징점과의 상대적인 거리( $d_m$ )가 가장 가까운  $M_1$ 부터  $M_5$ 까지 5개의 이웃 특징점( $M_i$ )를 결정하고, 상기 각각의 기준 특징점(M)과 5개의 이웃 특징점 사이의 상대적인 각도차( $\theta_m$ )와 용선의 수( $R_m$ )를 계산한다.

이때, 상기 기준 특징점(M)과 5개의 이웃 특징점( $M_i$ ) 사이의 상대적인 각도차( $\theta_m$ )는 도 4에 도시된 바와 같이, 상기 기준 특징점(M)의 방향을 기준으로 해서 반시계 방향각을 계산한다.

따라서, 상기와 같이 끝점과 분기점의 좌표값 및 방향정보로 구성된 일반적인 특징점 데이터에 추가적으로 가장 가까운 5개의 특징점 정보와 상기 5개의 이웃한 특징점 사이의 거리( $d_m$ ), 5개의 이웃한 특징점 사이의 상대적인 각도차( $\theta_m$ ), 5개의 이웃한 특징점 사이에 존재하는 용선의 수( $R_m$ )의 기하학적인 정보를 가지는 특징점 자료구조가 생성되며, 이와 같이 생성되는 특징점 자료구조의 데이터는 아래의 표 1과 같이 표시된다.

[표 1]

| M             | M <sub>n</sub> | $\Theta_{in}$ | D <sub>n</sub> | R <sub>n</sub> |
|---------------|----------------|---------------|----------------|----------------|
| 100,100,220,1 | 120,80,210,0   | 170           | 28,28          | 0              |
|               | 109,70,205,0   | 210           | 31,32          | 1              |
|               | 117,135,30,1   | 85            | 38,91          | 3              |
|               | 140,95,200,0   | 150           | 40,31          | 1              |
|               | 75,140,220,0   | 30            | 47,16          | 0              |
|               |                |               |                |                |
|               |                |               |                |                |
|               |                |               |                |                |
|               |                |               |                |                |
|               |                |               |                |                |

상기와 같이, USB 보안 토크에서, 사용자의 특징점 자료구조가 등록된 상태에서, 상기 호스트로 소정의 비교 지문 영상이 입력되면, 호스트에서는 비교 지문 영상에 대하여 상기 사용자 지문 등록 과정과 동일하게 전처리(S38), 특징점 추출(S40), 및 자료구조 생성(S42) 절차를 수행하여 상기 비교 지문 영상에 대한 특징점 자료구조를 생성하여 상기 USB 보안 토크으로 전송한다(S42).

이때, 상기 호스트에서 비교 지문 영상에 대하여 특징점을 추출하고 소정의 특징점 자료구조를 생성하는 과정은 상기 등록 지문 영상에 대한 특징점 추출 및 특징점 자료구조의 생성 과정과 동일하게 진행되어 상기 표 1과 같이 표시된다.

이에 따라서, USB 보안 토크에서는 기등록된 사용자의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점을 추출하고, 동일한 특징점을 기준으로 두 영상의 회전 및 전이에 대한 파라미터, 예컨대 비교해야 할 두 지문 영상사이의 회전각( $\Delta\theta$ ), 비교해야 할 두 지문 영상사이의 전이된 좌표양( $\Delta x, \Delta y$ )을 산출하여, 산출된 파라미터를 암호화하여 호스트로 전송한다(S44).

이때, 설정된 상기 호스트로 전송된 회전각( $\Delta\theta$ ) 및 전이량( $\Delta x, \Delta y$ )으로 산출되는 파라미터가 외부로 유출되더라도 상기 파라미터만으로는 USB보안 토크 등의 개인장치에 기등록된 상기 등록 지문을 추정할 수 없게 된다.

실제로, 상기 USB 보안 토크에서는 도 5에 도시된 바와 같이, 등록 지문의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점 쌍(M, M')을 추출한 후, 상기 동일한 특징점의 쌍(M, M')사이의 회전각( $\Delta\theta$ ) 및 전이량( $\Delta x, \Delta y$ )을 두 지문 영상의 좌표를 일치시키기 위한 보정 파라미터로 간주하여 소정의 파라미터를 계산한다. 특히, 상기와 같은 파라미터 계산은 곱셈 연산없이 단순한 덧셈 연산의 반복으로 가능하기 때문에, 하드웨어 자원이 제한적인 USB 보안 토크이나 스마트 카드와 같은 개인장치에서 동작 가능하다.

상기와 같이 암호화된 파라미터가 호스트로 전송되면 호스트에서 상기 암호화된 파라미터에 의해 상기 비교 지문 영상에 대한 특징점을 보정하여 USB 보안 토크으로 전송하고(S46), 이때 상기 USB 보안 토크에서는 보정된 비교 지문과 등록 지문의 특징점에 대한 점대칭 동작을 수행하여 등록 지문과 비교 지문의 일치 여부에 따라서 사용자 인증을 결정한다(S48).

이때, 상기 비교 지문 영상의 보정작업은 상기 파라미터 값을 이용하여 비교 지문의 좌표계를 등록 지문의 좌표계와 일치시킴으로써 수행되며, 이와 같은 호스트에서 보정작업을 수행하는 이유는 회전에 대한 보정을 수행 할 때 반복적인 곱셈 연산과 부동 소수점 연산이 필요하기 때문이며, 그 결과로 상기 비교 지문 영상에 대한 보정작업을 종래와 같이 스마트 카드나 USB 보안 토크와 같은 개인장치에서 수행할 때 발생하는 부동 소수점 연산을 고정 소수점 연산으로 변환하는 작업, 많은 곱셈 연산 수행, 오차 발생, 전력 소모량 증가 등의 문제점을 완전히 해소할 수 있게 된다.

특히, 두 개의 동일한 지문이 서로 정확하게 정렬되어 있다고 하더라도 특징점 추출시의 잡음, 지문 입력 시 지문 센서를 누르는 입력의 정도 때문에 발생하는 비선형 변환 등에 의해 특징점의 위치가 약간씩 달라지고, 심지어 존재하는 특징점이 누락되어 추출되거나, 존재하지 않는 의사 특징점이 추출될 수 있기 때문에, 상기 USB 보안 토크에서는 보정된 비교 지문과 등록 지문의 특징점에 대한 점대칭 동작을 수행할 때 오류를 없애기 위하여, 비교 지문의 특징점의 개수, 등록 지문의 특징점의 개수, 및 상기 특징점 각각에 대한 허용박스를 정해 놓은 후, 그 범위 안에서 비교 지문 특징점의 개수의 조합으로 두 지문 사이의 유사성을 판단하여 사용자 인증을 결정한다.

#### 발명의 효과

산출한 바와 같이 본 발명에 따른 저전력을 사용하는 개인장치용 지문 인식 방법은 다수의 메모리 등의 풍부한 하드웨어 자원을 구비한 호스트에서 등록 지문과 비교 지문의 특징점을 비교하고 보정하기 위한 공지의 부동 소수점 연산 및 곱셈 연산을 전적으로 수행하도록 하고, 스마트 카드나 USB 보안 토크와 같은 저전력을 사용하는 개인장치에서는 고정 소수점 연산(Fixed-point operation)의 반복만으로 지문 비교가 가능하도록 하기 때문에, 하드웨어 자원이 빈약하여 상기 부동 소수점 연산을 지원하지 않는 개인 장

치에서도 용이하게 적용할 수 있는 장점이 있다.

또한, 본 발명에 따른 지문 인식 방법이 적용되는 개인장치에서 산출한 파라미터는 별도로 암호화되어 등록지문 자체가 아닌 파라미터만을 호스트로 전송되기 때문에, 상기 개인장치에서 계산된 파라미터가 유출된다고 하더라도 파라미터만으로는 개인장치에 저장되어 있는 개인의 지문 정보를 유출할 수 없다는 보안상의 장점이 있다.

이상에서 설명한 것은 본 발명에 따른 저전력을 사용하는 개인장치를 지문 인식 방법을 실시하기 위한 하나의 실시예에 불과한 것으로서, 본 발명은 상기한 실시예에 한정되지 않고, 이하의 특허청구의 범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 범위까지 본 발명의 기술적 정신이 있다고 할 것이다.

#### (57) 청구의 범위

##### 청구항 1

호스트에서 사용자 인증을 위하여 등록하고자 하는 사용자의 지문 영상을 입력받아 전처리하여(S30) 지문의 특징점들을 추출한 후(S32), 추출된 특징점들간의 기하학적인 정보를 가지는 특징점 자료구조를 생성하는 단계(S34)와,

상기 호스트에서 생성된 특징점 자료구조를 개인장치에 등록하는 단계(S36)와,

상기 호스트로 비교 지문 영상이 입력되면 비교 지문 영상에 대한 특징점 자료구조를 생성하여 상기 개인장치로 전송하는 단계(S38, S40, S42)와,

상기 개인장치에서 기등록된 사용자의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점을 추출하고, 동일한 특징점을 기준으로 두 영상의 회전 및 전이에 대한 파라미터를 산출하여, 산출된 파라미터를 암호화하여 호스트로 전송하는 단계(S44)와,

호스트에서 상기 암호화된 파라미터에 의해 상기 비교 지문 영상에 대한 특징점을 보정하여 개인장치로 전송하는 단계(S46), 및

개인장치에서 보정된 비교 지문과 등록 지문의 특징점에 대한 점대칭 동작을 수행하여 사용자 인증을 결정하는 단계(S48)

로 이루어지는 것을 특징으로 하는 저전력을 사용하는 개인장치용 지문 인식 방법.

##### 청구항 2

제 1 항에 있어서, 상기 호스트에서 입력 지문 영상에 대한 특징점을 추출하고 특징점 자료구조를 생성하는 단계는,

입력 지문 영상으로부터 용선의 끝점과 분기점의 좌표값 및 방향정보로 구성된 특징점을 추출하는 단계와,

추출된 각각의 기준 특징점들에 대해서 상대적인 거리가 가장 가까운 5개의 이웃 특징점을 추출하는 단계, 및

상기 기준 특징점에 대하여 상기 기준 특징점과 5개의 이웃 특징점들 사이의 상대 각도, 상대 거리, 용선의 개수의 기하학적인 정보를 추가하여 특징점 자료구조를 생성하는 단계

로 이루어지는 것을 특징으로 하는 저전력을 사용하는 개인장치용 지문 인식 방법.

##### 청구항 3

제 1 항에 있어서, 상기 호스트에서 입력 지문 영상에 대한 특징점을 추출하는 단계는,

상기 파라미터 산출 단계 수행시의 특징점에 대한 탐색영역을 감소시키기 위해서 동일한 지문 영상을 2회 입력받아 특징점 추출작업을 2회 반복하여 얻은 두 지문 영상의 특징점 중에서 공통적으로 존재하는 특징점만을 추출하도록 된 것을 특징으로 하는 저전력을 사용하는 개인장치용 지문 인식 방법.

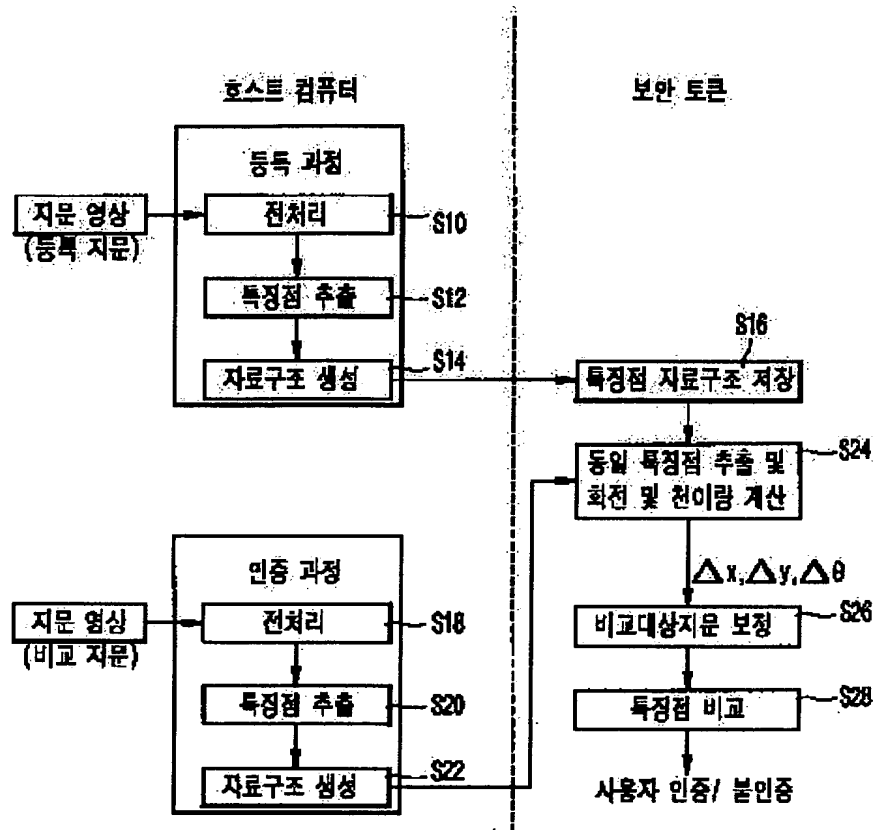
##### 청구항 4

제 1 항에 있어서, 상기 개인장치에서 기등록된 사용자의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점을 추출하고, 동일한 특징점을 기준으로 두 영상의 회전 및 전이에 대한 파라미터를 산출하여 암호화하는 단계에서는,

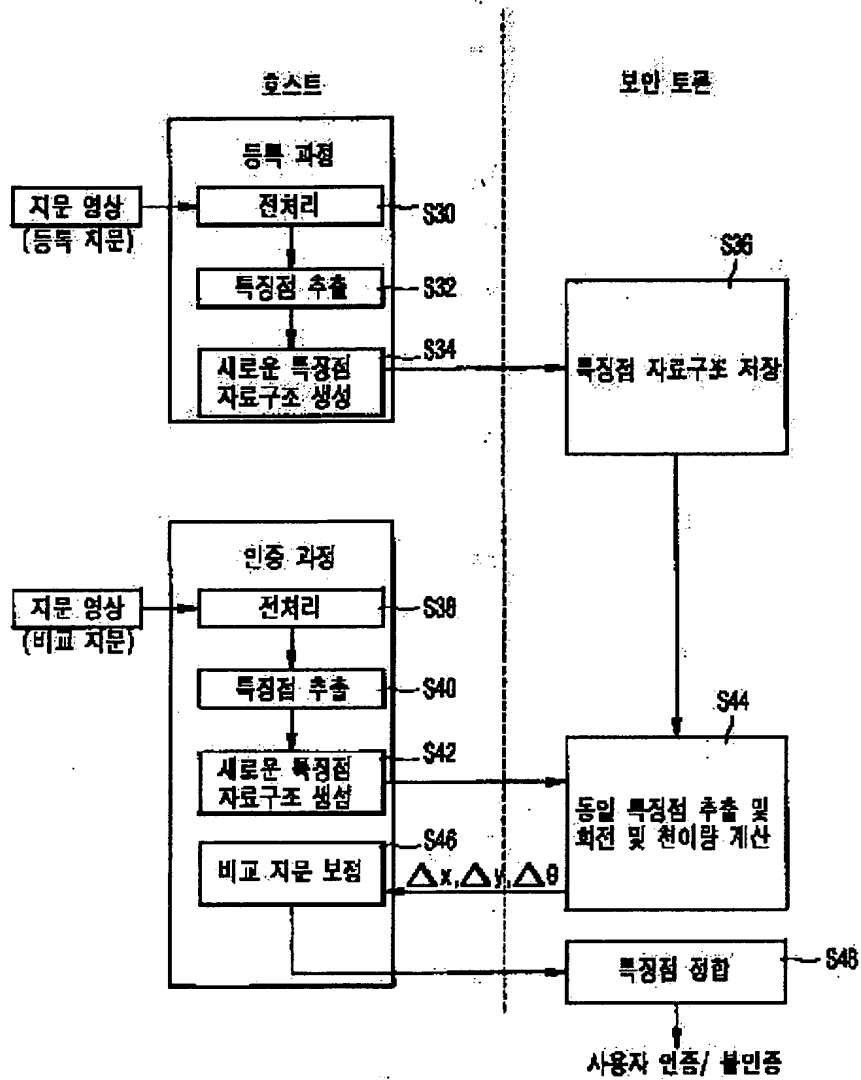
고정 소수점 연산 및 덧셈 연산만을 반복하여 등록 지문의 특징점 자료구조와 비교 지문 영상의 특징점 자료구조에서 동일한 특징점 쌍을 추출한 후, 상기 동일한 특징점의 쌍사이의 회전각 및 전이량을 두 지문 영상의 좌표를 일치시키기 위한 보정 파라미터로 간주하여 파라미터를 계산하도록 된 것을 특징으로 하는 저전력을 사용하는 개인장치용 지문 인식 방법.

도면

도면1

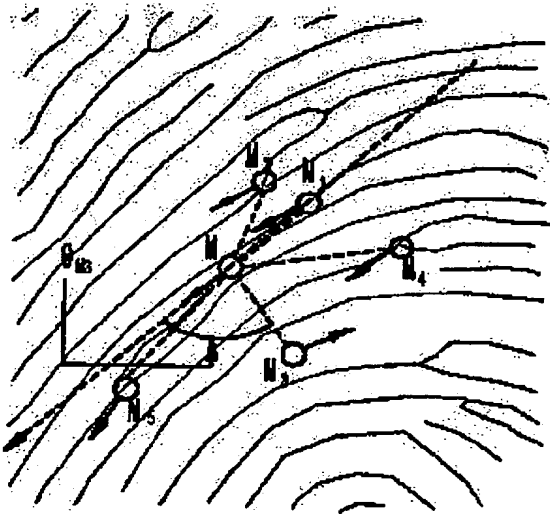


도면2

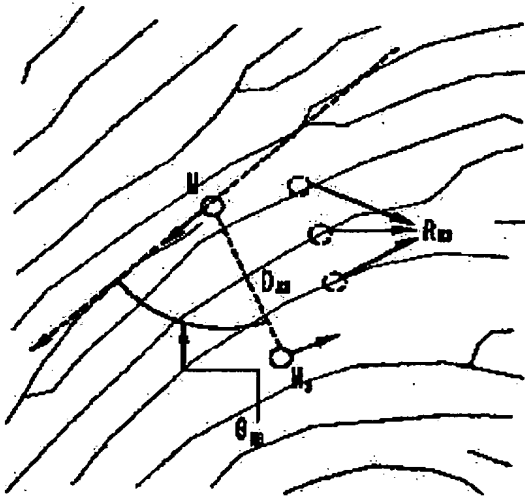




도 13



도 14



도 25

